KIBERFIRIBGARLIK TURLARI VA ULARNI ANIQLASH MEXANIZMLARI

Husanov Nodirbek Turdimurod o'g'li
O'zbekiston Respublikasi Ichki
ishlar vazirligi Akademiyasi
3-kurs 319-guruh kursanti
https://doi.org/10.5281/zenodo.24438679

Annotatsiya: Mazkur maqolada kiberfiribgarlikning mazmun-mohiyati, asosiy turlari hamda ularni aniqlashning zamonaviy mexanizmlari tahlil qilingan. Raqamli iqtisodiyot va axborot-kommunikatsiya texnologiyalarining jadal rivojlanishi sharoitida kiberfiribgarlikning ko'lami va murakkablashib borayotgan fishing (phishing), smishing, vishing, bank kartalari bilan bog'liq firibgarlik hamda kriptovalyutalar sohasidagi firibgarlik kabi keng tarqalgan turlar ko'rib chiqilgan. Tadqiqot natijasida kiberfiribgarlikka qarshi kurashda texnik, tashkiliy va huquqiy choralarni kompleks qo'llash zarurligi asoslab berilgan hamda kiberxavfsizlikni kuchaytirishga qaratilgan amaliy tavsiyalar ishlab chiqilgan.
Kalit so'zlar: kiberfiribgarlik, kiberxavfsizlik, fishing (phishing), smishing, vishing, ijtimoiy muhandislik, sun'iy intellekt, mashinaviy o'qitish, ko'p omilli autentifikatsiya, axborot xavfsizligi.

Abstract: This article analyzes the essence of cyber fraud, its main types, and modern detection mechanisms. In the context of the rapid development of the digital economy and information and communication technologies, the study examines the increasing scale and sophistication of widespread forms of cyber fraud, including phishing, smishing, vishing, bank card fraud, and cryptocurrency-related fraud. The research substantiates the necessity of applying integrated technical, organizational, and legal measures to combat cyber fraud and provides practical recommendations aimed at strengthening cybersecurity.
Keywords: cyber fraud, cybersecurity, phishing, smishing, vishing, social engineering, artificial intelligence, machine learning, multi-factor authentication, information security.

Аннотация: В данной статье рассматриваются сущность кибермошенничества, его основные виды и современные механизмы выявления. В условиях стремительного развития цифровой экономики и информационно-коммуникационных технологий проанализированы масштабы и усложнение наиболее распространённых видов кибермошенничества, включая фишинг, смишинг, вишинг, мошенничество с банковскими картами и мошенничество, связанное с криптовалютами. По результатам исследования обоснована необходимость комплексного применения технических, организационных и правовых мер в борьбе с кибермошенничеством, а также предложены практические рекомендации, направленные на повышение уровня кибербезопасности.
Ключевые слова: кибермошенничество, кибербезопасность, фишинг, смишинг, вишинг, социальная инженерия, искусственный интеллект, машинное обучение, многофакторная аутентификация, информационная безопасность.

Raqamli texnologiyalar va axborot-kommunikatsiya tizimlarining jadal rivojlanishi jamiyatning deyarli barcha sohalarida raqamlashtirish jarayonlarini tezlashtirdi. Elektron tijorat, masofaviy bank xizmatlari, mobil to'lov tizimlari hamda davlat xizmatlarining elektron shaklga o'tishi fuqarolar va tashkilotlar uchun keng qulayliklar yaratgan bo'lsa-da, kiberxavfsizlik bilan bog'liq yangi tahdidlarning yuzaga kelishiga ham sabab bo'ldi. Ana shunday tahdidlarning eng dolzarblaridan biri kiberfiribgarlik bo'lib, u shaxsiy ma'lumotlarni noqonuniy qo'lga kiritish, moliyaviy mablag'larni o'g'irlash yoki foydalanuvchilarni aldash orqali moddiy va ma'naviy zarar yetkazishga qaratilgan noqonuniy harakatlarni o'z ichiga oladi. So'nggi yillarda kiberfiribgarlik usullari tobora murakkablashib, sun'iy intellekt, ijtimoiy muhandislik va avtomatlashtirilgan dasturiy vositalardan foydalanish orqali amalga oshirilmoqda. Natijada nafaqat oddiy foydalanuvchilar, balki banklar, davlat tashkilotlari va yirik kompaniyalar ham ushbu tahdidlarning nishoniga aylanmoqda. Bu holat kiberfiribgarlikni erta aniqlash, xavflarni baholash va samarali himoya mexanizmlarini ishlab chiqish zaruratini yanada kuchaytirmoqda.

Kiberfiribgarlikka qarshi kurash faqat texnik vositalarni joriy etish bilangina cheklanmaydi. Mazkur yo'nalishda huquqiy tartibga solish, foydalanuvchilarning raqamli savodxonligini oshirish, tashkilotlarda axborot xavfsizligi siyosatini takomillashtirish hamda zamonaviy tahliliy texnologiyalarni qo'llash muhim ahamiyat kasb etadi. Xususan, sun'iy intellekt va mashinaviy o'qitish algoritmlariga asoslangan firibgarlikni aniqlash tizimlari shubhali operatsiyalarni real vaqt rejimida aniqlash imkonini bermoqda.

Mazkur tadqiqotning **maqsadi** kiberfiribgarlikning asosiy turlarini tizimli tahlil qilish, ularni aniqlashning zamonaviy mexanizmlarini o'rganish hamda kiberfiribgarlikning oldini olish bo'yicha amaliy tavsiyalar ishlab chiqishdan iborat.

Tadqiqotning vazifalari quyidagilardan iborat:

- kiberfiribgarlik tushunchasi va uning asosiy turlarini ilmiy adabiyotlar asosida tahlil qilish;
- zamonaviy kiberfiribgarlik usullarining o'ziga xos xususiyatlarini aniqlash;
- firibgarlikni aniqlashda qo'llanilayotgan texnologik va tashkiliy mexanizmlarni baholash;
- kiberfiribgarlikning oldini olish bo'yicha amaliy tavsiyalar ishlab chiqish.

Tadqiqot obyekti sifatida internet tarmog'i va axborot-kommunikatsiya texnologiyalarida sodir etilayotgan kiberfiribgarlik holatlari tanlandi. **Tadqiqot predmeti** esa kiberfiribgarlikni aniqlash mexanizmlari, axborot xavfsizligi vositalari hamda ularning amaliy qo'llanilishidan iborat. Tadqiqotda tizimli tahlil, qiyosiy tahlil, statistik ma'lumotlarni umumlashtirish, ilmiy adabiyotlarni o'rganish va mantiqiy xulosa chiqarish **usullari**dan foydalanildi.

Mazkur maqolaning ilmiy ahamiyati kiberfiribgarlik turlarini zamonaviy yondashuv asosida tizimlashtirish, ularni aniqlashning ilg'or texnologiyalarini tahlil qilish hamda amaliyot uchun foydali tavsiyalar ishlab chiqishga qaratilganligi bilan belgilanadi. Tadqiqot natijalari davlat organlari, moliya institutlari, axborot texnologiyalari sohasi mutaxassislari hamda kiberxavfsizlik bo'yicha ilmiy izlanish olib borayotgan tadqiqotchilar uchun amaliy ahamiyat kasb etishi mumkin.

Kiberfiribgarlik (cyber fraud) — bu axborot-kommunikatsiya texnologiyalari, internet tarmoqlari va raqamli platformalardan foydalangan holda shaxsiy ma'lumotlar, moliyaviy

mablag'lar yoki boshqa turdagi raqamli aktivlarni noqonuniy qo'lga kiritishga qaratilgan kiberjinoyat turi hisoblanadi. An'anaviy firibgarlikdan farqli ravishda kiberfiribgarlik masofaviy amalga oshirilishi, katta miqyosda tarqalishi va zamonaviy texnologiyalardan foydalanishi bilan ajralib turadi. Raqamli xizmatlarning keng tarqalishi, elektron to'lov tizimlari va onlayn savdo platformalarining rivojlanishi kiberfiribgarlik sodir etish imkoniyatlarini oshirdi. Bugungi kunda kiberjinoyatchilar foydalanuvchilarning ishonchidan foydalanish, zaif autentifikatsiya tizimlarini chetlab o'tish hamda zararli dasturiy vositalar yordamida maxfiy ma'lumotlarni qo'lga kiritish kabi usullardan foydalanmoqda. Kiberfiribgarlikning asosiy maqsadi odatda moliyaviy foyda olish bo'lsa-da, ayrim hollarda shaxsiy ma'lumotlarni yig'ish, identifikatsiya ma'lumotlarini o'g'irlash yoki tashkilotlarning axborot tizimlariga noqonuniy kirish ham ko'zda tutiladi. Shu sababli kiberfiribgarlik nafaqat moliyaviy, balki axborot xavfsizligi va shaxsiy daxlsizlikka ham jiddiy tahdid hisoblanadi. Endi bir necha kiberfiribgarlik turlarini ko’rib chiqamiz.

Fishing — kiberfiribgarlikning eng keng tarqalgan shakllaridan biri bo'lib, foydalanuvchilarni aldash orqali maxfiy ma'lumotlarni qo'lga kiritishga qaratilgan hujum usulidir. Bunda hujumchilar odatda banklar, davlat tashkilotlari yoki mashhur xizmat ko'rsatuvchi kompaniyalar nomidan soxta elektron xatlar, veb-saytlar yoki xabarlar yuboradi. Fishing hujumlarining asosiy maqsadi foydalanuvchining login va parollari, bank karta ma'lumotlari, shaxsiy identifikatsiya ma'lumotlari kabi axborotlarni qo'lga kiritishdan iborat. Zamonaviy fishing hujumlari sun'iy intellekt yordamida (Deepfake) yanada takomillashib, matnlarning ishonchliligi va hujumlarning aniqligini oshirmoqda.

Smishing (SMS phishing) — fishing hujumlarining mobil aloqa vositalari orqali amalga oshiriladigan turi hisoblanadi. Ushbu usulda kiberjinoyatchilar foydalanuvchilarga SMS xabarlar yuborib, zararli havolalarga o'tishni yoki maxfiy ma'lumotlarni taqdim etishni talab qiladi. Ko'pincha bunday xabarlar bank operatsiyalari, sovrinli aksiyalar, yetkazib berish xizmatlari yoki davlat xizmatlari nomidan yuboriladi. Foydalanuvchi havolaga kirganida soxta sahifaga yo'naltirilishi va uning ma'lumotlari hujumchilar qo'liga o'tishi mumkin.

Vishing (Voice phishing) — telefon qo'ng'iroqlari orqali amalga oshiriladigan kiberfiribgarlik turi. Bunda hujumchilar o'zlarini bank xodimi, huquqni muhofaza qiluvchi organ vakili yoki boshqa ishonchli tashkilot vakili sifatida tanishtirib, foydalanuvchidan maxfiy ma'lumotlarni olishga harakat qiladi. Vishing hujumlarida inson psixologiyasiga ta'sir o'tkazish, qo'rquv yoki shoshilinch qaror qabul qilish holatini yaratish kabi ijtimoiy muhandislik usullaridan keng foydalaniladi.

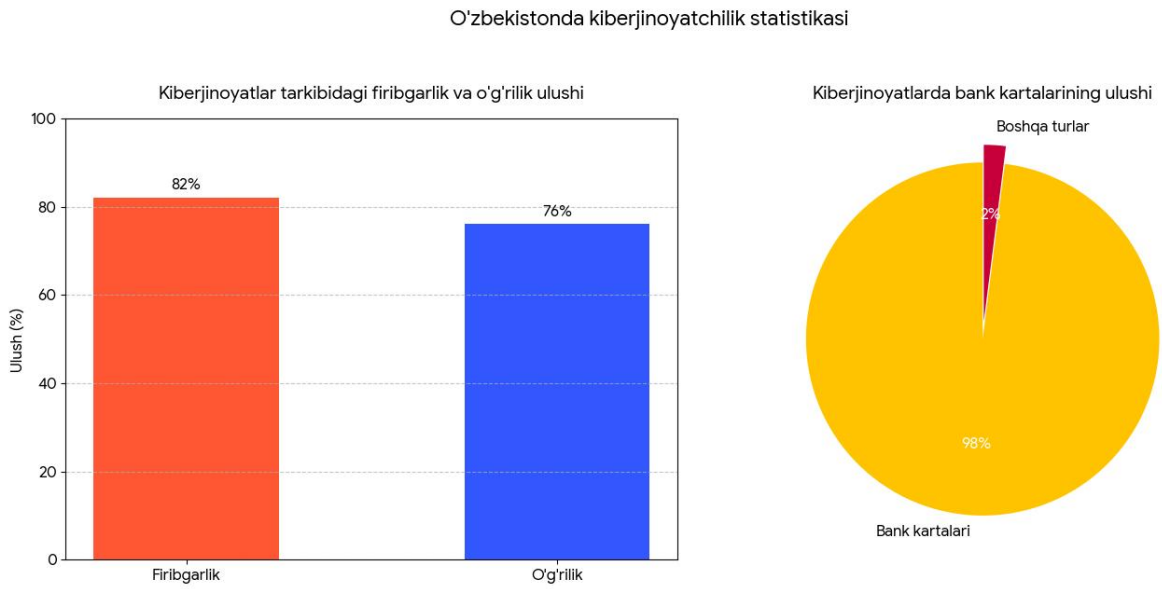
Ijtimoiy muhandislik — texnik zaifliklardan ko'ra inson omiliga ta'sir qilish orqali amalga oshiriladigan hujumlar majmuasidir. Ushbu usulda kiberjinoyatchilar foydalanuvchining ishonuvchanligi, e'tiborsizligi yoki yetarli axborotga ega emasligidan foydalanadi. Ijtimoiy muhandislik fishing, smishing va vishing kabi ko'plab kiberfiribgarlik usullarining asosini tashkil etadi. Mazkur hujumlarga qarshi kurashishda texnik himoya bilan bir qatorda foydalanuvchilarning kiberxavfsizlik bo'yicha bilimlarini oshirish muhim ahamiyatga ega.

Bank kartalari bilan bog'liq kiberfiribgarlik — elektron to'lov tizimlarining rivojlanishi bilan keng tarqalgan tahdidlardan biridir. Ushbu turdagi firibgarliklarda bank karta raqamlari, amal qilish muddati, CVV kodi (bank kartasining himoya kodi) yoki internet-banking hisob ma'lumotlari noqonuniy qo'lga kiritiladi. Bunday hujumlar ko'pincha fishing

sahifalari, zararli dasturlar yoki ijtimoiy muhandislik usullari yordamida amalga oshiriladi. Bank tashkilotlari tomonidan **ko'p bosqichli autentifikatsiya** va **tranzaksiyalarni monitoring qilish** tizimlarining joriy etilishi ushbu xavflarni kamaytirishga xizmat qilmoqda.

Kriptovalyuta bozorining rivojlanishi yangi turdagi kiberfiribgarlik shakllarining paydo bo'lishiga sabab bo'ldi. Ushbu turdagi firibgarliklar soxta investitsiya loyihalari, qalbaki kriptovalyuta platformalari, phishing hujumlari va raqamli hamyonlarni buzish orqali amalga oshiriladi. Kriptovalyuta operatsiyalarining ko'pincha qaytarib bo'lmasligi va anonimlik xususiyatlari kiberjinoyatchilar uchun qo'shimcha imkoniyatlar yaratadi. Shu sababli foydalanuvchilarning raqamli moliyaviy savodxonligini oshirish va xavfsizlik choralarini kuchaytirish muhim hisoblanadi.

2026-yilning hozirgi davriga qadar sodir etilgan kiberfiribgarliklar bo‘yicha aniq yakuniy statistika hali e’lon qilinmagan bo‘lsa-da, rasmiy ma’lumotlarga ko‘ra, mamlakatda qayd etilgan **jami firibgarlik jinoyatlarining 82 foizi va o‘g‘rilik jinoyatlarining 76 foizi aynan kibermakonda** sodir etilmoqda. Oxirgi besh-olti yillik ko‘rsatkichlar tahlil qilinganda, O‘zbekistonda kiberjinoyatlar bo‘yicha murojaatlar soni **48 baravarga oshgani** va jami kiberjinoyatlar soni **62 mingdan ortgani** ma'lum qilingan.



Kibermakon orqali jismoniy va yuridik shaxslarga yetkazilgan jami moddiy zarar miqdori **2 trillion so‘mdan oshgan** (umumiy hisobda esa 3,7 trillion so‘mdan ko‘p). Kiberjinoyatlarning mutlaq aksariyat qismini (**98 foizini**) bank kartalari bilan bog‘liq o‘g‘rilik va firibgarliklar tashkil qiladi. Jinoyatlarning **60 foizi** zararli havola (fishing) va ilovalar yuborish, **16 foizi** esa turli aldovlar (qo‘ng‘iroqlar yoki SMS-kod so‘rash) orqali amalga oshirilmoqda.

Raqamli texnologiyalarning jadal rivojlanishi bilan bir qatorda kiberfiribgarlik usullari ham murakkablashib bormoqda. An'anaviy xavfsizlik yondashuvlari ko'pincha zamonaviy kiberhujumlarni aniqlashda yetarli samaradorlik bermaydi. Shu sababli kiberfiribgarlikni aniqlashda sun'iy intellekt, mashinaviy o'qitish, katta hajmdagi ma'lumotlarni tahlil qilish hamda avtomatlashtirilgan monitoring tizimlariga asoslangan zamonaviy mexanizmlardan foydalanish dolzarb ahamiyat kasb etmoqda. Kiberfiribgarlikni aniqlash tizimlarining asosiy vazifasi foydalanuvchi xatti-harakatlari, moliyaviy operatsiyalar, tarmoq faolligi va boshqa raqamli izlarni tahlil qilish orqali shubhali holatlarni aniqlashdan iborat. Bunday tizimlar real

vaqt rejimida xavflarni baholash, firibgarlik ehtimolini aniqlash va zararni kamaytirish imkonini beradi.

Sun'iy intellekt (Artificial Intelligence — AI) texnologiyalari kiberfiribgarlikni aniqlash sohasida eng istiqbolli yo'nalishlardan biri hisoblanadi. Sun'iy intellekt algoritmlari katta hajmdagi ma'lumotlarni tezkor qayta ishlash, foydalanuvchilarning odatiy xatti-harakatlarini o'rganish va noodatiy faoliyatlarni aniqlash imkonini beradi. **Mashinaviy o'qitish (Machine Learning — ML) usullari** yordamida tizimlar avvalgi firibgarlik holatlari asosida o'qitilib, yangi tahdidlarni aniqlash qobiliyatiga ega bo'ladi. Masalan, bank operatsiyalarini tahlil qilishda mashinaviy o'qitish algoritmlari foydalanuvchining odatiy tranzaksiya xususiyatlarini aniqlaydi va odatdagidan farqli bo'lgan harakatlarni shubhali sifatida belgilaydi. Mashinaviy o'qitishning asosiy yo'nalishlariga quyidagilar kiradi:

- **Nazorat ostida o'qitish (Supervised Learning)** — oldindan belgilangan firibgarlik holatlari asosida yangi holatlarni aniqlash;
- **Nazoratsiz o'qitish (Unsupervised Learning)** — ma'lumotlardagi yashirin bog'liqlik va anomaliyalarni topish;
- **Chuqur o'qitish (Deep Learning)** — murakkab naqshlarni aniqlash uchun neyron tarmoqlardan foydalanish.

Firibgarlikni aniqlash tizimlari tashkilotlarning axborot xavfsizligini ta'minlashda muhim vositalardan biridir. Ushbu tizimlar moliyaviy operatsiyalar, foydalanuvchi faoliyati va tarmoq harakatlarini doimiy ravishda monitoring qiladi. Bank va moliya sohasida bunday tizimlar quyidagi omillarni tahlil qiladi:

- tranzaksiya hajmi va chastotasi;
- foydalanuvchining joylashuvi;
- qurilma ma'lumotlari;
- to'lov amalga oshirilayotgan vaqt;
- avvalgi operatsiyalar tarixi.

Agar tizim odatiy xatti-harakatlardan keskin farq qiluvchi holatni aniqlasa, qo'shimcha tekshiruv o'tkazishi yoki operatsiyani vaqtincha bloklashi mumkin. Bu esa moliyaviy zararlarning oldini olishga yordam beradi.

Anomaliyalarni aniqlash (Anomaly Detection) kiberfiribgarlikni aniqlashning samarali usullaridan biri hisoblanadi. Ushbu yondashuvda tizim foydalanuvchi yoki tarmoqdagi odatiy faoliyat modelini shakllantiradi va undan chetga chiqadigan harakatlarni aniqlaydi. Masalan, foydalanuvchi odatda ma'lum hududdan kichik hajmdagi to'lovlarni amalga oshirsa, qisqa vaqt ichida boshqa davlatdan katta miqdordagi tranzaksiya amalga oshirilishi shubhali holat sifatida baholanishi mumkin. Anomaliyalarni aniqlashda quyidagi algoritmlardan foydalaniladi:

- klasterlash algoritmlari;
- statistik tahlil usullari;
- neyron tarmoqlar;
- qaror daraxtlari;
- assotsiativ tahlil algoritmlari.

Ko'p omilli autentifikatsiya (MFA) foydalanuvchi shaxsini tasdiqlashning zamonaviy xavfsizlik mexanizmlaridan biridir. Ushbu usul foydalanuvchidan faqat parolni emas, balki qo'shimcha tasdiqlash omillarini ham talab qiladi. MFA odatda quyidagi omillarga asoslanadi:

- **bilish omili** — parol yoki PIN-kod;

- **egalik omili** — mobil qurilma, token yoki autentifikatsiya ilovasi;
- **biometrik omil** — barmoq izi, yuzni aniqlash yoki ovoz orqali tasdiqlash.

Ko'p omilli autentifikatsiya parollar o'g'irlangan taqdirda ham ruxsatsiz kirish ehtimolini sezilarli darajada kamaytiradi.

Xulq-atvor biometrikasi foydalanuvchilarning raqamli muhitdagi o'ziga xos harakatlarini tahlil qilishga asoslangan texnologiyadir. Ushbu mexanizm insonning qurilmadan foydalanish uslubini, klaviaturada yozish tezligini, sichqoncha harakatlarini yoki mobil qurilmadan foydalanish odatlarini o'rganadi. Mazkur texnologiyaning afzalligi shundaki, u foydalanuvchidan qo'shimcha harakat talab qilmasdan shubhali faoliyatni aniqlashi mumkin. Masalan, hisob egasidan farqli bo'lgan xatti-harakatlar aniqlansa, tizim qo'shimcha tekshiruv talab qiladi.

Katta hajmdagi ma'lumotlar (Big Data)ni tahlil qilish texnologiyalari kiberfiribgarlikning murakkab shakllarini aniqlashda muhim rol o'ynamoqda. **Big Data** vositalari yordamida millionlab tranzaksiyalar, tarmoq hodisalari va foydalanuvchi faoliyati qisqa vaqt ichida tahlil qilinadi. Bunday yondashuv tashkilotlarga tahdidlarni oldindan aniqlash, xavf darajasini baholash va samarali himoya strategiyalarini ishlab chiqish imkonini beradi.

Kiberfiribgarlikning doimiy ravishda takomillashib borishi ushbu tahdidga qarshi kurashishda kompleks yondashuvni talab qiladi. Faqatgina texnik himoya vositalaridan foydalanish yetarli bo‘lmay, **tashkiliy, huquqiy va ijtimoiy choralar**ni ham birgalikda amalga oshirish zarur. Kiberfiribgarlikning oldini olish tizimi axborot tizimlarini himoyalash, foydalanuvchilarning raqamli savodxonligini oshirish hamda zamonaviy xavfsizlik mexanizmlarini joriy etishga asoslanadi.

Kiberfiribgarlikka qarshi kurashda texnik himoya vositalari muhim o‘rin tutadi. Zamonaviy axborot tizimlarida xavfsizlikni ta’minlash uchun turli dasturiy va apparat yechimlardan foydalaniladi. Asosiy texnik himoya vositalariga quyidagilar kiradi:

- **Ko‘p omilli autentifikatsiya (MFA)** — foydalanuvchi hisoblarini himoyalash va ruxsatsiz kirishlarning oldini olish imkonini beradi;
- **Shifrlash texnologiyalari (Encryption)** — maxfiy ma’lumotlarni uzatish va saqlash jarayonida ularning xavfsizligini ta’minlaydi;
- **Antivirus va zararli dasturlardan himoyalash tizimlari** — viruslar, josuslik dasturlari va boshqa zararli vositalarni aniqlashga yordam beradi;
- **Tarmoq xavfsizligi vositalari** — xavfsizlik devorlari (Firewall), hujumlarni aniqlash va oldini olish tizimlari (IDS/IPS) orqali tarmoq faoliyatini nazorat qiladi;
- **Zaxira nusxalash tizimlari (Backup)** — ma’lumotlar yo‘qolishi yoki buzilishi holatlarida ularni qayta tiklash imkonini beradi.

Bundan tashqari, dasturiy ta’minotlarni muntazam yangilab borish va xavfsizlik zaifliklarini bartaraf etish kiberhujumlarning oldini olishda muhim ahamiyatga ega. Kiberfiribgarlikning oldini olishda tashkilotlarda samarali axborot xavfsizligi siyosatini shakllantirish zarur. Texnologik himoya vositalari qanchalik rivojlangan bo‘lmasin, inson omili yetarli darajada nazorat qilinmasa, xavfsizlik zaiflashishi mumkin. **Tashkiliy choralar** quyidagilarni o‘z ichiga oladi:

- axborot xavfsizligi bo‘yicha ichki siyosat va me’yorlarni ishlab chiqish;
- xodimlarni muntazam ravishda kiberxavfsizlik bo‘yicha o‘qitish;
- foydalanuvchilarning kirish huquqlarini cheklash va nazorat qilish;

- xavfsizlik hodisalariga javob berish rejalarini ishlab chiqish;
- muntazam xavfsizlik auditi va monitoringini amalga oshirish.

Xodimlarning kiberxavfsizlik bo‘yicha bilimlarini oshirish ayniqsa muhimdir, chunki ko‘plab kiberfiribgarlik holatlari insonlarning e’tiborsizligi yoki aldov usullariga ishonishi natijasida yuzaga keladi.

Kiberfiribgarlikka qarshi samarali kurashish uchun **huquqiy baza**ni takomillashtirish muhim yo‘nalishlardan biridir. Kiberjinoyatlarning xalqaro xususiyatga ega ekanligi sababli davlatlar o‘rtasidagi hamkorlik va yagona huquqiy yondashuvlarni shakllantirish talab etiladi. Huquqiy choralar quyidagilarni o‘z ichiga oladi:

- kiberjinoyatlar uchun javobgarlik choralarini belgilash;
- shaxsiy ma’lumotlarni himoya qilish bo‘yicha qonunchilikni takomillashtirish;
- elektron to‘lovlar xavfsizligini tartibga solish;
- kiberjinoyatlarni tergov qilish mexanizmlarini rivojlantirish;
- xalqaro tashkilotlar va davlatlar bilan axborot almashinuvini yo‘lga qo‘yish.

Huquqiy mexanizmlarning samaradorligi texnik vositalar va tashkiliy choralar bilan uyg‘unlashgandagina yuqori natija beradi. Kiberfiribgarlikning ko‘plab shakllari inson omiliga asoslanganligi sababli foydalanuvchilarning kiberxavfsizlik madaniyatini oshirish muhim profilaktik choradir. Foydalanuvchilarga quyidagi xavfsizlik qoidalarini o‘rgatish zarur:

- noma’lum havolalar va fayllarni ochmaslik;
- shaxsiy ma’lumotlar va bank rekvizitlarini begona shaxslarga bermaslik;
- murakkab va takrorlanmaydigan parollardan foydalanish;
- ikki bosqichli autentifikatsiyani yoqish;
- shubhali elektron xatlar va xabarlarni tekshirish;
- onlayn xizmatlardan foydalanishda rasmiy manbalarga murojaat qilish.

Aholining raqamli savodxonligini oshirish kiberfiribgarlikning oldini olishda eng samarali uzoq muddatli strategiyalardan biri hisoblanadi.

Kiberfiribgarlik tahdidlarining murakkabligi sababli unga qarshi kurash faqat bitta yo‘nalish doirasida amalga oshirilishi mumkin emas. Samarali himoya strategiyasi texnologik yechimlar, tashkiliy boshqaruv, huquqiy mexanizmlar va inson omilini hisobga olgan holda shakllantirilishi lozim. Kompleks strategiya quyidagi asosiy yo‘nalishlarni qamrab oladi:

- xavflarni muntazam baholash;
- ilg‘or aniqlash texnologiyalaridan foydalanish;
- davlat va xususiy sektor hamkorligini rivojlantirish;
- kiberxavfsizlik bo‘yicha mutaxassislar tayyorlash;
- jamiyatda xavfsiz raqamli xulq-atvorni shakllantirish.

Shunday qilib, kiberfiribgarlikning oldini olish texnik, tashkiliy va huquqiy choralarni yagona tizim sifatida amalga oshirishni talab qiladi. Faqat kompleks yondashuv orqali raqamli muhitda xavfsizlik darajasini oshirish va kiberjinoyatlar oqibatlarini kamaytirish mumkin.

Tadqiqot davomida kiberfiribgarlikning asosiy turlari, ularning yuzaga kelish sabablari hamda aniqlashning zamonaviy mexanizmlari tahlil qilindi. Raqamli texnologiyalarning rivojlanishi bilan birga fishing, smishing, vishing, ijtimoiy muhandislik va moliyaviy firibgarlik kabi kiberxavflar ham kengayib bormoqda. Kiberfiribgarlikka qarshi kurashishda sun’iy intellekt, mashinaviy o‘qitish, anomaliyalarni aniqlash, ko‘p omilli autentifikatsiya kabi zamonaviy texnologiyalar muhim ahamiyat kasb etadi. Shu bilan birga, samarali himoya uchun

texnik vositalar bilan bir qatorda tashkiliy va huquqiy choralarni ham qo‘llash zarur. **Xulosa qilib aytganda,** kiberfiribgarlikning oldini olishda ilg‘or texnologiyalarni joriy etish, foydalanuvchilarning kiberxavfsizlik bo‘yicha bilimlarini oshirish va kompleks himoya strategiyalarini ishlab chiqish raqamli muhit xavfsizligini ta’minlashning muhim omillaridan biridir.

Foydalanilgan adabiyotlar:

1. O‘zbekiston Respublikasi Konstitutsiyasi. — Toshkent: O‘zbekiston Respublikasi qonunchilik ma’lumotlari milliy bazasi, 2023.
2. O‘zbekiston Respublikasining “Kiberxavfsizlik to‘g‘risida”gi Qonuni. O‘RQ–764-son, 2022-yil 15-aprel.
3. O‘zbekiston Respublikasining “Shaxsga doir ma’lumotlar to‘g‘risida”gi Qonuni. O‘RQ–547-son, 2019-yil 2-iyul.
4. O‘zbekiston Respublikasining “Axborotlashtirish to‘g‘risida”gi Qonuni. O‘RQ–560-II-son, 2003-yil 11-dekabr.
5. O‘zbekiston Respublikasi Prezidentining “Raqamli O‘zbekiston – 2030” strategiyasini tasdiqlash to‘g‘risida”gi Farmoni. PF–6079-son, 2020-yil 5-oktabr.
6. International Telecommunication Union (ITU). Global Cybersecurity Index (GCI). Geneva: ITU, 2021.
7. European Union Agency for Cybersecurity (ENISA). ENISA Threat Landscape Report. European Union Agency for Cybersecurity, 2023.
8. National Institute of Standards and Technology (NIST). Cybersecurity Framework (CSF) 2.0. Gaithersburg: NIST, 2024.
9. Anderson, R. Security Engineering: A Guide to Building Dependable Distributed Systems. 3rd ed. Wiley, 2020.
10. Stallings, W., Brown, L. Computer Security: Principles and Practice. 4th ed. Pearson, 2018.
11. Whitman, M. E., Mattord, H. J. Principles of Information Security. 7th ed. Cengage Learning, 2021.
12. Hadnagy, C. Social Engineering: The Science of Human Hacking. 2nd ed. Wiley, 2018.
13. Ngai, E. W. T., Hu, Y., Wong, Y. H., Chen, Y., Sun, X. The application of data mining techniques in financial fraud detection: A classification framework and an academic review of literature. Decision Support Systems. 2011. Vol. 50(3). P. 559–569.
14. Abdallah, A., Maarof, M. A., Zainal, A. Fraud detection system: A survey. Journal of Network and Computer Applications. 2016. Vol. 68. P. 90–113.
15. Sarker, I. H. Machine Learning: Algorithms, Real-World Applications and Research Directions. SN Computer Science. 2021. Vol. 2. Article 160.
16. Federal Bureau of Investigation (FBI). Internet Crime Report. 2023.
17. O‘zbekiston Respublikasi Prezidentining rasmiy veb-sayti, 2026, https://president.uz.